

NPS 56-81-002

② LEVEL 1

AD A100013

# NAVAL POSTGRADUATE SCHOOL

Monterey, California



DTIC  
ELECTE  
JUN 10 1981  
S B

BATTLE OF WITS  
Synthesizing and Extrapolating from NPS Research  
on Strategic Military Deception

Katherine L. Herbig, Donald C. Daniel

January 1981

Final Report for Period October 1979 - 30 June 1980

Approved for public release; distribution unlimited.

Prepared for: Office of The Director of Net Assessment  
The Pentagon  
Washington, D.C. 20301

DTIC FILE COPY

81 6

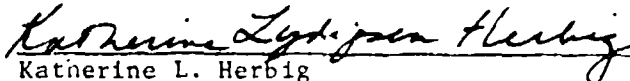
10 000


NAVAL POSTGRADUATE SCHOOL  
Monterey, California

Rear Admiral John J. Ekelund  
Superintendent

David A. Schradly  
Acting Provost

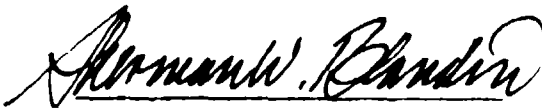
The work reported herein was supported by the Office of the Director of Net Assessment, Department of Defense. Reproduction of all or part of this report is authorized.


  
Katherine L. Herbig  
Assistant Professor of  
National Security Affairs

  
Donald C. Daniel  
Associate Professor of  
National Security Affairs

Reviewed by:

Released by:

  
Sherman W. Blandin  
Acting Chairman  
Department of National  
Security Affairs

  
William M. Tolles  
Dean of Research

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER NPS-56-81-002	2. GOVT ACCESSION NO. AD-A100 013 9	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Battle of Wits: Synthesizing and Extrapolating from NPS Research on Strategic Military Deception.		5. TYPE OF REPORT & PERIOD COVERED 1 October 1979 - 30 June 1980
7. AUTHOR(s) Katherine L. Herbig and Donald C. Daniel		6. PERFORMING ORG. REPORT NUMBER
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940		8. <del>XXXXXX</del> OR GRANT NUMBER(s)
11. CONTROLLING OFFICE NAME AND ADDRESS Office of The Director of Net Assessment The Pentagon Washington, D.C. 20301		10. PROGRAM ELEMENT PROJECT, TASK AREA & WORK UNIT NUMBERS
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)		12. REPORT DATE January 1981
		13. NUMBER OF PAGES 65
		15. SECURITY CLASS. (of this report) Unclassified
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE
16. DISTRIBUTION STATEMENT (of this Report) Approved for public release; distribution unlimited		
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)		
18. SUPPLEMENTARY NOTES		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number) Military Deception      Misperceptions Deception                Strategic Deception Intelligence Failure      Cover Counter Deception		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number)  The main findings of a group research project on strategic deception at the Naval Postgraduate School are summarized. The discussion includes the following topics: defining deception, tracing the deception process, judging the likelihood of deception, the difficulties of deception, advantages of the deceiver, the advantages of the offensive in deception, the impact of astuteness, doing counterdeception, and conclusions.		

DD FORM 1 JAN 73 1473

EDITION OF 1 NOV 65 IS OBSOLETE  
S N 0102-014-6601

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

BATTLE OF WITS

Synthesizing and Extrapolating from NPS Research  
on Strategic Military Deception

by

Katherine L. Herbig

Donald C. Daniel

Accession For	
NTIS GRA&I	<input checked="checked" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution/	
Availability Codes	
Avail and/or	
Dist	Special
A	

Naval Postgraduate School  
Monterey, California  
January 1981

## SUMMARY

Main findings in this report are given in the brief "headlines" which introduce each section. The text explains and elaborates on these headlines. Here we present the headlines with only the minimum explanation necessary to summarize our results.

1. Defining deception. Deception is a broad concept which encompasses and goes beyond the ideas of cover, lying, and artifice. In our view deception constitutes a deliberate misrepresentation of reality done to gain a competitive advantage. There are two basic variants of deception: the ambiguity-increasing type, and the misleading type.

2. The deception process. Strategic deception is a process of encoding, transmitting, and decoding messages. There are two categories of messages in the process. These are: micromessages, i.e., the meaning of each signal in a deception; and macromessages, the implications for his own action a target derives from the totality of signals he receives.

3. The likelihood of deception. There are two groups of factors conditioning the likelihood of deception: personal qualities, and aspects of the particular military situation. Personal factors include the impact of culture, the nature of the political system, the presence or absence of deception in doctrine, and past experience. Military factors include the importance of the outcome, the level of confidence in victory, and the degree of uncertainty in an encounter.

4. The difficulties of deception. There are many points at which deception can in theory fail. It is a fragile and risky

enterprise. Accidents may foil the transmission of deceptive signals; undesired interpretations may result from the psychological or organizational peculiarities of the target; circumstances may prevent a target's acting on a deceptive interpretation.

5. The advantages of the deceiver. In practice deceptions usually succeed. They aid the deceiver's cause even if they do not go strictly according to plan. Despite inevitable accidents and uncertainties, deceptions succeed because adversaries must seek out intelligence on their opponents, thereby risking deception; processes of human perception tend to favor the deceiver; the uncertainties inherent in hostile competition often forgive a deceiver's mistakes; and the cost of deception failure is usually low.

6. The advantage of the offensive. Being on the offense provides a better position for succeeding at deception than being on the defense. This is particularly true in the early stages of an attack. Defensive deception, however, can be effective under the right circumstances. Among these circumstances, the most important is anticipation of the need to begin a deceptive scenario soon enough.

7. The impact of astuteness. Deceivers who act astutely can enhance the advantages they already enjoy from the dynamics of deceptive interaction. By applying acumen to see through the target's eyes, by assessing his goals, by calibrating the degree of time pressure exerted, and by following some basic deception rules, deceivers can improve their chances of success.

8. The importance of feedback. In strategic deception feedback is the deceiver's most valuable asset. It forms the basis of the most astute deceptions. Feedback may be indirect, i.e., observational, or direct; the latter is preferable, more powerful, and more difficult to achieve.

9. Doing counterdeception. Countering deception is extremely difficult, but success need not always require detecting deception. Merely sensitizing analysts to deception has its own problems. Acumen seems a desirable trait in counterdeception analysts. The use of alternative hypotheses and attempts to elicit confirmation of suspected deception from the adversary are recommended techniques of counterdeception. By increasing the likelihood of ambush a target can deter or foil deception without actually detecting it.

10. Conclusions. Strategic deception is a powerful tool, particularly in the hands of an astute practitioner. The danger of being confused about or misled in one's assessment of a military situation, and the increased time and analytical energy demanded to deal with potential deception, are unavoidable and often severe disadvantages for the target of deception.

CHAPTER ONE  
INTRODUCTION

This report presents the main findings and conclusions of the NPS Deception Working Group. By design the group reflected a variety of academic disciplines and intellectual interests. It consisted of two political scientists, an historian, a physicist, a psychologist, an electrical engineer/systems scientist, and a specialist in the application of psychological insights and systematic research methods to the intelligence process. Though each investigator worked more or less independently when writing his or her individual study, all assumed deception to be well-suited for multi-disciplinary inquiry and all interacted regularly with one another in order to test and refine ideas.

The group's intent was to illuminate the nature of deception, its processes, and factors which condition when one resorts to and succeeds at deception. In order to narrow the focus and facilitate access to relatively concrete historical data, the group oriented its efforts to the study of strategic military deceptions. These involve large numbers of individuals and organizations as perpetrators and victims of deception, including the national command authorities on both sides of the deception interaction. They are relatively long-term deceptions, recurring over the course of weeks or months. Their stakes are very high in that they can affect the outcomes of wars or large-scale front-level campaigns



as opposed to tactical deceptions, which affect the outcome of battles or local engagements.

The group's overall research strategy was twofold. The members sought to develop a common view of deception, its primary elements, and their relation. Each investigator then applied or tailored existing social and engineering science frameworks, hypotheses, and principles to the problem of strategic deception. The end result was the production of seven studies completed between Fall 1979 and Spring 1980. Four specifically focussed on the application of game, communication, organization, and systems theories. The remaining three were more eclectic, drawing from historical cases and documents and from concepts and principles contained in a variety of academic sources, especially political science and psychological literature on decision-making and perceptual and cognitive processes. It is from these seven studies and from some earlier preliminary point papers that we draw the findings and conclusions for this report. (See figure 1 which identifies the investigators, their academic disciplines or specialties, and titles of their final studies).

The group's research strategy was consistent with the fact that there were no well-established basic concepts or theoretical priors associated with the topic. The starting point for the group's conceptualization consisted of rudimentary insights drawn from personal experience, initial consideration of classic cases such as the Normandy and Pearl Harbor attacks, and the study of now declassified World War II and post-war documents

TABLE 1

NPS Deception Working Group Members and Studies\*

<u>NAME</u>	<u>DISCIPLINE/SPECIALTY</u>	<u>STUDY</u>
Donald C. Daniel Katherine L. Herbig	Political Scientist Historian	Propositions on Military Deception
Richards J. Heuer	Intelligence Specialist	Cognitive Factors in Deception and Counterdeception
Theodore L. Sarbin	Psychologist	On the Psychological Analysis of Counter- deception
Ronald G. Sherwin	Political Scientist	Assessing the Value of an Organizational Approach to Strategic Deception
William Reese	Physicist	(1) Deception Within a Communication Frame- work  (2) Deception in a Game Theoretic Frame- work
Paul Moose	Electrical Engineer/ Systems Scientist	A Systems Model for Deception

---

\*All studies are contained in D.C. Daniel, K.L. Herbig et al., Multidisciplinary Perspectives on Military Deception (Technical Report 56-80-012; Monterey, CA: Naval Postgraduate School, 1980).

setting down "lessons learned" from the wartime practice of deception. The contribution of all these sources consisted mainly of rules for the conduct of successful deception (Be credible; Keep the fact of deception a secret; Pay attention to detail; and the like). While of some utility for orientating us to factors influencing success or failure, these rules also proved misleading. They were simplistic, and they unduly narrowed our perspectives. To some extent it was necessary to "unlearn" them so as to fully appreciate the complexity of the deception phenomenon.

There are three sections to this report. The first deals with the conceptual issues of defining deception, identifying its variants, and outlining and characterizing the deception process. The second centers on issues of practice. It focuses on factors conditioning resort to deception, reasons for deception's success or failure, the advantage of the offensive for a deceiver, questions of deceiver astuteness, the importance of feedback, and counter-deception difficulties and options. The third section concludes this report and offers our thoughts on the utility of deception.

## CHAPTER TWO

### CONCEPTS

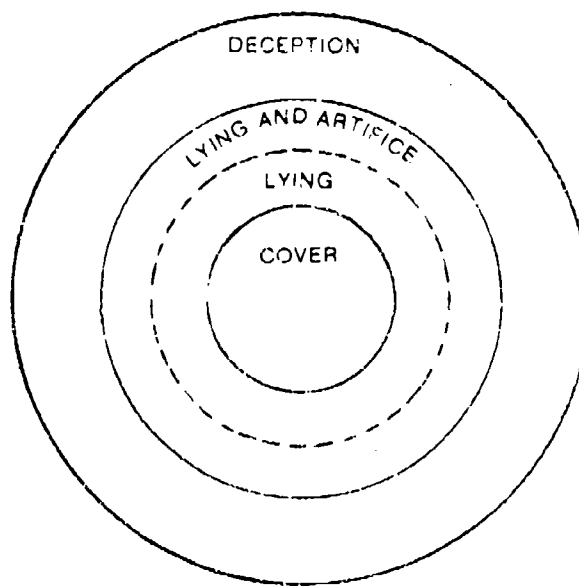
#### Defining Deception

Deception is a broad concept which encompasses and goes beyond the ideas of cover, lying, and artifice.

As in any research area, that of deception required bounding the concept and analytically distinguishing it from related terms. Several members of the Deception Working Group addressed these problems in early point papers. Explicit or implicit in all papers was the view that deception constituted a deliberate misrepresentation of reality done to gain a competitive advantage. The Daniel and Herbig study built on this definition, and offered Figure 1 to illustrate that deception is a broad concept encompassing several subsidiary ideas.

At the figure's center is cover, the military term for secret-keeping and camouflage. It embodies deception's negative side because it entails negating knowledge of the truth. Cover is at the heart of deception because, no matter what his other goals, a deceiver wishes to protect a secret, be it information about an already existing reality (e.g., the capabilities of one's military systems) or an intended reality (such as the scenarios for their use).

**Figure 1**  
**Deception's Subsidiary Concepts**



The concept "lying" encompasses that of "cover." Not only does a liar hold back the truth; he also acts to deflect his victim away from it, thus highlighting deception's positive side. Liars create and perpetuate falsities and seek to draw a victim's attention to them. In a narrow sense, to lie simply means making a statement the text of which is untrue, but in a broader sense it can also involve manipulating the context surrounding the statement in order to enhance its veracity. This is what is meant by artifice, an important element of nearly all strategic deceptions.

Just as lying subsumes cover, so does deception subsume lying in both of its textual and contextual senses. The terms are often used interchangeably, but deception and lying are not exact synonyms. Lying looks primarily to one side of the interaction between a liar and his audience. It stresses the actions of the teller of falsehoods. Deception is a term of wider scope because it also stresses the reactions of the receiver of falsehoods. Someone whose false tale is not believed is still a liar, but he has not deceived. One does not fail at lying because the audience is not convinced, but one does fail at deception if the audience does not believe the lie. Eventually almost all deceptions are exposed as events unfold; thus the trick for the deceiver is to insure his lies are accepted long enough to benefit him.

The question of benefits is important because they are a necessary ingredient of deception as we see it. In our view, to be labeled deception an act must be done to gain a

competitive advantage. This means, in effect, that there are three goals in any deception. The immediate aim is to condition a target's beliefs; the intermediate aim is to influence his actions; and the ultimate aim is for the deceiver to benefit from the target's actions. Deceptions are often credited with success when only the first goal is achieved, but to evaluate the actual impact deception has on the course of events, its success should properly be measured against the third goal.

### Variants

There are two variants of deception, and they may be viewed as end points on a continuum. The variant the deceiver intends may not be that which results as an outcome.

Early in their deliberations, all members of the group accepted that there were two variants to deception, each operating in different ways and producing different effects. The less elegant variety is the "ambiguity producing" or A type. Here a deceiver acts to confuse a target by confronting him with at least two choices as to what the truth may be. One of these choices may be the truth itself, whose indicators the target cannot completely hide. The greater the number of compelling alternatives, the smaller the possibility a target may by chance settle on the true one as the basis for his actions. In order to be compelling, it is necessary only that a deceiver's lies be plausible enough and consequential enough to the target's well-being that he cannot ignore them.

A deceiver can benefit from an "A" deception in two ways. Hoping to reduce ambiguity by awaiting additional information, a target may delay decision, thereby surrendering the initiative to the deceiver and giving him wider latitude to marshal resources. If the deceiver can insure that the situation remains confusing, then the target may be forced to spread resources thinly to cover all important contingencies. He thereby reduces the resistance a deceiver can expect at any one point.

In contrast to deceptions increasing ambiguity, there is a second, more complicated, category which we labelled "misleading" or M type. They reduce ambiguity and fasten a victim's mind to one (false) version of the truth. Whereas in A deceptions the deceiver simply aims to have a target not reject as untrue one or more alternatives to the truth, the aim in the M variant is to have the target reject the truth itself and all alternatives to it except the one which suits the deceiver. Not only must the lie be plausible, it must be so attractive, so convincing, that the victim is willing to concentrate the bulk of his operational resources on one contingency, thereby maximizing the deceiver's chances for prevailing on all others. This variant is particularly attractive in situations where the deceiver believes he can keep most indicators of the truth from ever reaching the target in the first place.

There are at least three types of misleading deceptions. The first or M-1 variety seeks to have a victim accept as true that which he is already inclined to believe. It is probably the easiest of the M deceptions to carry through to success.



Conversely, the most difficult of the M deceptions is the M-2 variety. Here the deceiver swims against the tide of the victim's predispositions. He seeks to have the victim believe that which the victim is inclined to doubt or view as false. The M-3 version concerns those cases where the victim's predispositions (prior to the commencement of the deception) are not directly relevant to or predictive of what the victim comes to accept as true.

Although the two variants of deception, M type and A type, are conceptually distinct and can be initiated with different intentions in the deceiver's mind, in practice their effects often coexist or shade into one another as the deception evolves. In the latter case the direction of change generally appears to be from M type to A type. Deceptions planned to mislead a target into choosing one possibility may degenerate and instead increase uncertainty if the target resists or postpones making the choice the deceiver intends.

How one categorizes a particular deception partly depends on the perspective one takes. The variants can differ whether viewed from the deceiver's intentions or from the effect they ultimately have on the target. Strategic deceptions seem to be most often intended to mislead, since this form offers the largest potential payoff to the deceiver. However, one would expect pure misleading deceptions to obtain rarely because they require a target to be so sure of a false alternative that he stakes all on preparing for it. Prudent commanders seldom do this. They develop contingency preparations for other conceivable

alternatives. Thus it is useful to consider the outcomes of the two variants as a continuum between convinced misdirection at the one pole and utter confusion, in which all looks equally likely, at the other. The Barbarossa deception (misleading Stalin about the German attack in June 1941) seems to be an unusually strong example of misdirection, while immediately before D-Day Fortitude South (the deception associated with the Normandy landing) would fall perhaps three-fourths of the way toward the misdirection pole. In the Barbarossa case the Germans ultimately built on Stalin's expectation that the Third Reich would never attack the USSR without first issuing an ultimatum. This "ultimatum strategy," according to Whaley, "served to eliminate ambiguity, making Stalin quite certain, very decisive, and wrong."<sup>1</sup> (Emphasis is original.) In the Fortitude case Hitler and many of his generals thought in late May and early June 1944 that the main Allied cross-Channel invasion would come at Calais, but they continued to consider a range of invasion site possibilities along the English Channel coast, including Normandy.

In sum, there are two deception variants which differ in their intended effects. One seeks to increase a target's uncertainty and the other to decrease it. It seems useful to view these variants as end points in a spectrum with the outcome of actual deception usually falling between the two extremes.

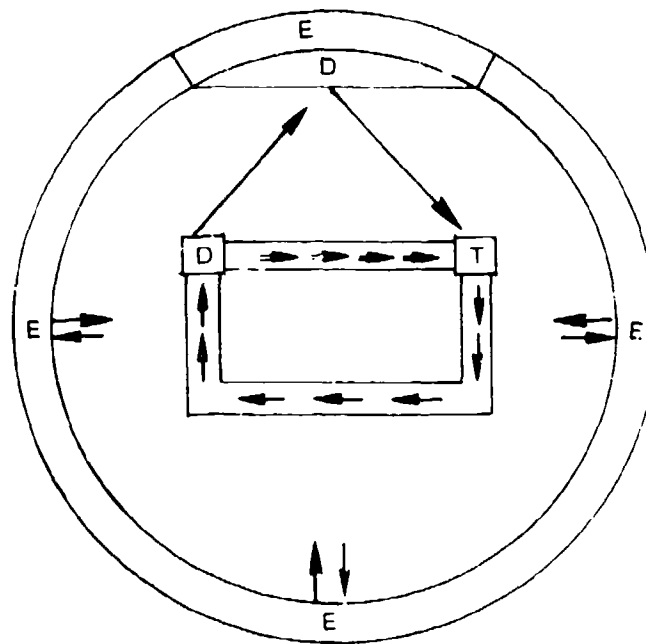
## Process






Strategic deception is a process of encoding, transmitting, and decoding messages. There are two categories of messages in the process.

Elements of the deception process. Figure 2 models the basic or generic elements of the deception process as understood by the group. It identifies a deceiver, his victim or target, communication channels linking them together, and signals transmitted within the channels. It also illustrates that each of these elements affects and is affected by environmental factors, some of which are deliberately manipulated by the target as part of his deception.

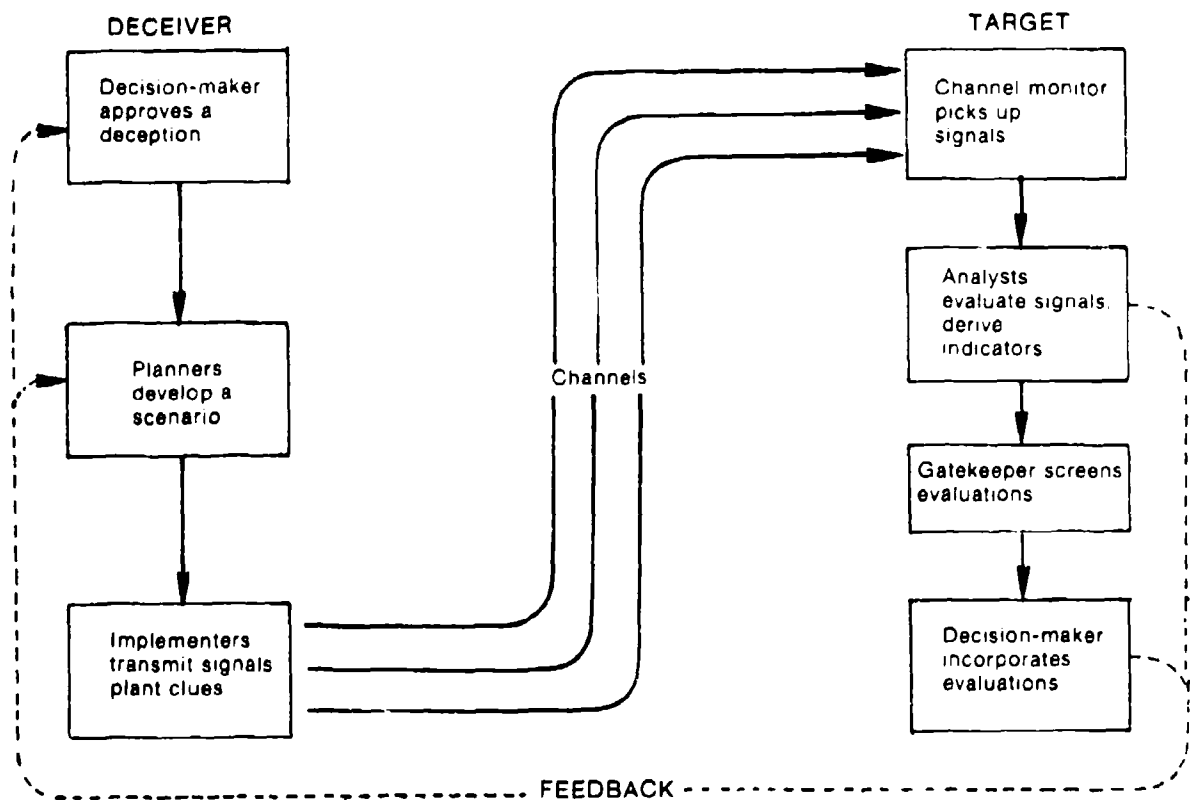
Figure 3 elaborates on the deceiver and target elements. The deceiver's side consists of decision-makers, planners, and implementers. Regardless of who had the inspiration, a deception does not begin until a decision-maker agrees to it. The historical record reveals that wide-ranging strategic deceptions such as Fortitude or Barbarossa are cleared only by the highest authorities, but given their many responsibilities, they were unable to devote much time to planning and implementation. During World War II such tasks were assigned to small cadres in intelligence-gathering and covert action organizations as well as military staffs. These groups were often not a normal part of the civilian or military bureaucracy but rather, like the famous London Controlling Section, were specially formed during the

**FIGURE 2**  
**Simplified View of the Deception Process**



-  = Deceiver
-  = Target
-  = Channels
-  = Signals
-  = Feedback
- E** = Environment
- E<sub>D</sub>** = Portion of environment manipulated by deceiver

**Figure 3**  
**Deceiver and Target Elements in the Process of Deception**



war and disbanded or severely cut back at its conclusion. On an as-needed basis, implementers temporarily coopted regular military personnel who generated false radio traffic, set up deceptive camouflage, simulated large troop movements or encampments and the like. National political leaders, high level diplomats, civil servants, businessmen, and news reporters also often played starring roles in strategic deceptions.

The initial target of a military deception is usually a state's intelligence organization. It consists of channel monitors who seek out and collect information and analysts who coordinate and evaluate it. Gatekeepers within intelligence agencies and command staffs screen the information and analyses, and determine what is actually forwarded to civilian or military authorities--the ultimate deception targets. Presumably relying on information received, these leaders make the strategic or tactical decisions which the deceivers seek to influence.

The links or "channels" between deceivers and targets make deception possible, and their variety is unlimited. A channel could be a newspaper monitored by the target, his reconnaissance satellites, electronic intercept systems, diplomats, or spies. Through these channels are transmitted signals, physical phenomena which can be observed or sensed by the target. A signal may be a news article on the activities of a general, a reduction in military radio traffic, or a staged unloading of ships. To a target preparing to repel an amphibious attack, these signals are (planted) clues of the attacker's interest. When put together they indicate that the attack will not soon

occur since the general expected to lead it is away on other business, radio traffic is too sparse to support an attack, and ships preparing to carry out an imminent landing usually onload rather than offload goods.

As illustrated in Figure 2, the flow of signals in a strategic deception is not only from deceiver to target. Because these deceptions occur over weeks or months, the deceiver has time to monitor his target's statements and actions in order to ascertain the effects of the deception while it is still ongoing. The statements and actions constitute return signals--termed "feedback"--which provide the deceiver a basis for modulating his activities. In a successful deception, of course, the target is not aware that his actions and statements constitute this kind of feedback. Should the target realize it, the stage is set for a further permutation in the deception process, entrapment of the deceiver by his victim. By using the feedback channels to send deceptive signals to his enemy, the target becomes the deceiver and the deception channels become feedback for this new layer of deception.

Environmental variables affecting the deception process are almost infinite in number since they include any factor exogenous to the set made up of deceiver, target, their communication links and signals. As yet there is no framework for systematically accounting for or investigating environmental factors. Even if such a framework existed, it is the deception group's experience that it would be difficult to apply, for, while some critically important idiosyncratic factors are generally and

easily identifiable in historical analyses, the impact of other variables is often impossible to isolate, much less measure.

A clearly distinguishable and often important group of environmental variables is the subset manipulated or controlled by the deceiver. Engaging in artifice, he may act, e.g., to silence sources passing on to the target information inconsistent with the deception, or he may seek to increase the stature of individuals or organizations on the target's side whose views would further acceptance of the deception.

Deception as a process. Implied in the above discussion is a view of deception as a process of encoding, transferring, and decoding messages where there are two categories of messages. The message feature is evident in the example used earlier. In it the target was concerned with repelling an expected amphibious attack, and the deceiver transmitted three signals to shape the target's estimate of the attack's timing: a news article on a general's activities, reduced radio traffic, and a staged unloading of ships. Each signal contained its own micromessage to the effect that "the general is away," "radio traffic is too sparse," and "ships are offloading." The micromessages become important when the target properly interprets and conjoins them, for they convey the overarching macromessage--"an amphibious attack will not soon occur"--devised by the deceiver for the target's consumption. In a misleading deception only one macromessage is intended. In the ambiguity-producing variant, a number of macromessages may be generated, each with its own micromessage subset.



The overall process of deception, then, is one where the deceiver knows the truth he wants to protect; he concocts one or more alternative truths (or macromessages) for dissemination to the target; he deduces what micromessages will serve as indicators of the "truth"; he converts the micromessages into signals or physical referents which he transfers or makes available to the target. Starting with the physical referents the target reverses the process performed by the deceiver up to the point of inducing the candidate or candidates for the "truth" concocted by the deceiver. As the deception progresses, the target's reaction to micromessages can serve as return signals to the deceiver, giving him the opportunity to adjust his activities and make them more effective.

## CHAPTER 3

### PRACTICE

#### Likelihood of Deception

There are two groups of factors conditioning the likelihood of deception: personal qualities and aspects of the particular military situation.

Two groups of factors influence the likelihood of military deception: those which characterize situations confronting an actor and those which actors bring to a situation by virtue of previous conditioning or personal predilection. The factors may operate independently or in combination with one another. It is difficult to establish a priori which group is more important. The second set probably has greater impact.

Of the first group, high stakes situations can certainly influence willingness to deceive. When outcomes are critical, adversaries are encouraged to make use of every capability, every advantage, to insure victory or stave off defeat.

Resort to deception can be particularly compelling if decision-makers are not fully confident of a situation's outcome because of their own military weaknesses. Desiring to compensate for them, they seek through some ruse to induce an enemy to lower his guard, dilute his strength, or concentrate his forces on the wrong objective. Plans Bodyguard and Barclay, for the invasions of Normandy and Sicily, e.g., both reflected the concern that

until a beachhead is secured, amphibious landings are highly vulnerable to being pushed back into the sea. From the attacker's perspective, it is thus imperative to assure that the defender's response capability be as limited as possible. Weaker in mechanized forces, Hitler similarly wanted to limit Allied response to Case Yellow, the May 1940 push into France. He convinced the Allies that his main thrust would be through Holland and Belgium. While the British and French massed in that direction, the Wehrmacht's primary offensive was actually far to the south at Sedan. It then turned toward the channel encircling the cream of the Allied armies. The Dunkirk evacuation meant that the bulk of these would fight again, but for France the war was lost.

Even when optimistic of the outcome of a situation, an actor may be attracted to deception as one way to lower costs. The wish to avoid being viewed as an aggressor has inspired many a nation to fabricate evidence that its victim actually fired the first shot. The wish to avoid human or material losses has resulted in schemes such as the British plan in 1943 to protect their bombers attacking Peenemunde. Though confident this German rocket facility could be destroyed, the British sought to minimize their own casualties. They succeeded in deflecting German fighters from their bomber streams by convincing the enemy's air defense that Berlin was the target instead.

Situations characterized by uncertainty can also induce deception. In those circumstances, actors often seek to mislead or confuse in order to keep their options open and to test the reaction to alternative policies. A state undecided as to

whether to attack another, for instance, may still wish to be ready to do so. This was the case prior to the last-minute Soviet decision to invade Czechoslovakia. Having its troops "exercise" in border areas for the greater part of the summer allowed the USSR to proceed with preparations for an invasion while not openly committing itself to this step. It also allowed the Soviets to save face if they decided not to attack. After all, the Czechs might have backed down, making attack unnecessary, or they might have rallied the overwhelming support of the world community, making the invasion option even more unattractive.

In any of these situations, not all states or individuals would resort to deception. Actors bring their own conditioned responses, their own predilections, to the problems they face. We see at least five factors possibly at play here.

First, there may be "deception styles" which vary from culture to culture that would account for the differences in when and how nations use deception. The intriguing thought that some societies' values or expected modes of personal interaction condition individuals to understand and succeed at deception is to our knowledge largely unexplored.

Studies of the Chinese have shown that deception has traditionally been part of Chinese military strategy because it is so available in the cultural norms. The Chinese assume interpersonal deception will and should occur constantly between individuals as a means of protecting face by deflecting too-threatening truths.<sup>2</sup> Since at least the doctrines of Sun Tzu

in the fourth century B.C., the Chinese have long prized victories gained by undermining through deception an adversary's desire or ability to give battle. The potential link between a culture's expectation for interpersonal truthfulness or deceptiveness and that culture's resort to military deception is not yet well formed, but it remains suggestive. For example, does a country like the United States, with a culture noted for the openness, even the naiveté of its interpersonal interactions, find strategic deception uncongenial to its habitual ways of thinking?

It is conceivable that by studying cultural norms we may learn to predict how nations will employ deception in military contexts. One analysis, e.g., compares national patterns in the deceptive practices of the Soviets and the Chinese. It describes the Soviets' use of the "false war scare" to overawe opponents, their penchant for "disinformation," and their efforts to induce overestimation of their military capabilities. This contrasts with the Chinese preference for the "deep lure," the multiple stratagem, and the anticipation of the enemy's intentions through acumen.<sup>3</sup> This type of work suggests that by expanding systematic comparison of national "deception styles," one can isolate patterns that could alert counter-deception analysts sooner to the deceptive ploys of a particular culture.

A second conditioning factor may be the nature of the political system in which an actor operates. This argument is developed in a paper by Herbert Goldhamer in which he contends that deception may be more common in states

where political leaders take a strong, central role in military decision-making. His work implies that politics either attracts individuals prone to deception or conditions individuals to practice it. As a corollary to his general argument, he adds that a tendency to deceive is particularly prevalent in dictatorships and authoritarian regimes. He reasons that the "secrecy and total control available [in these governments], and the reduced inhibitions that accompany such exercise of power, facilitate and provide incentives for the exercise of craft, cunning, and deception."<sup>4</sup>

Paralleling Goldhamer's perspective are two closely related factors. One is the bureaucratic imperative that organizations trained for particular tasks will seek to perform them. The other is the psychological trait that people tend to think in terms of what is available or familiar to them. These phenomena suggest that military deception is likely to occur if a nation maintains an apparatus to plan and organize deception, or if its military preserves, passes on, or at least debates a doctrine for deception. Conversely, nations having no such apparatus or doctrine, or which allow them to atrophy, must overcome the inertia involved in creating or revivifying them--a situation characteristic of America's early strategic deception efforts in World War Two.

Finally, there is the issue of a person's own predilection to deception. It is clear that even within the same cultural or organizational setting, individuals differ in this regard. Some leaders relish deception, others put up with it, still

others resist it. Why this is so remains largely unexplored. Barton Whaley searched his historical data for evidence of a "deceptive personality type," a group of attributes or experiences that would account for these difference, but could find none. At present we must be content to observe that personal reactions to deception are at least self-consistent. That is, a commander who has appreciated and relied on deception in the past is likely to do so again. Winston Churchill was an early proponent of deception in World War I and encouraged its elaboration again twenty years later; Douglas MacArthur used serial deceptions in his campaign across the Pacific, and succeeded with deception again at Inch'on in Korea. In following the good advice to "know thine enemy," a nation might be well served to evaluate its opponent's experience with deception.

### Difficulties of Deception

There are many points at which deception can in theory fail. It is a fragile and risky enterprise.

Succeeding at deception seems unlikely when we consider the many difficulties which plague deceivers. New problems attend each of the three stages of a deception, i.e., causing a target to receive signals, to interpret them as intended, and to act on them in a way which benefits the deceiver. These problems generate considerable uncertainty which seems intrinsic to doing deception.

The amateurish formulation and transmission of clues is unlikely to fool an alert adversary. Even when signals are flawlessly crafted and implemented, however, a deceiver may be undone by accidents in transmission which he cannot predict or prevent.

Figure 4 depicts accidents which may befall a signal after a deceiver releases it into a channel and loses control over it. In this figure the deception consists of eight clues arranged at the top; the deceiver intends his target to put them together like a puzzle to reach a deceptive conclusion. Clue 1 is shown sent repeatedly in order to depict the variety of possibilities for its fate.

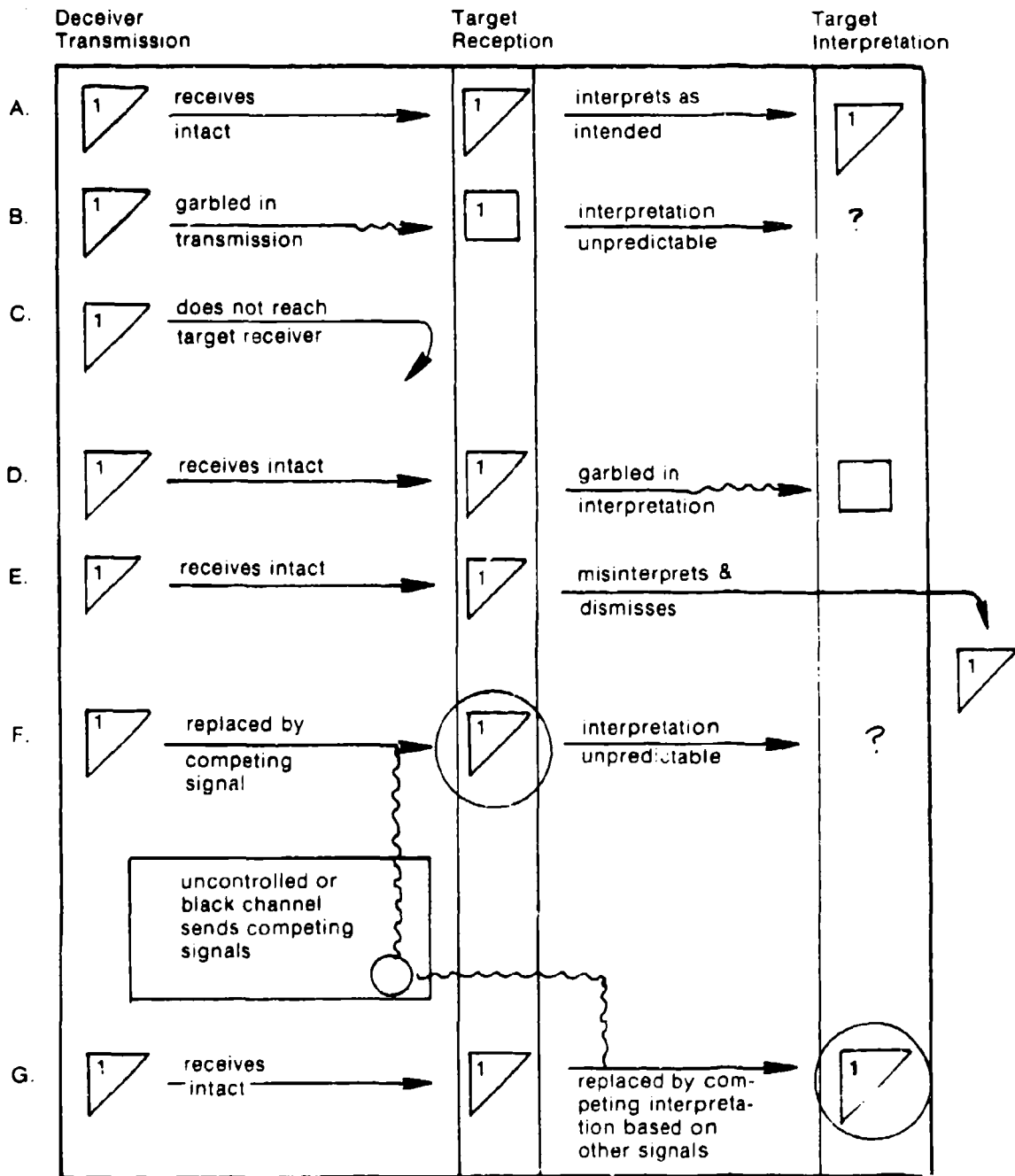
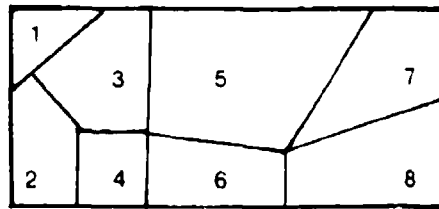
Signal A represents the deceiver's fondest hope: the Target receives and interprets the signal as the deceiver intended, so an identical shape appears in the transmission, reception, and interpretation columns. In Signal B the clue is modified or garbled in the channel, and the target receives a different signal, the square. How he will interpret this unexpected signal the deceiver cannot know. Signal C is deflected in transmission and never reaches the target receiver.

Signals D and E depict smooth transmission and reception of signals which are then damaged when the target interprets them to find their micromessages. In D target analysts garble the interpretation, i.e., they do not understand it as it was intended. In E analysts do not see the significance of the signal and dismiss it as trivial or irrelevant.



FIGURE 4

Possible Results of Transmitting a Deceptive Signal



The last two signals represent the effects of white, (uncontrolled) or black, (unknown) channels on a deceiver's signals. In F a competing signal, a circle, overwhelms the clue in transmission and replaces it in the target's receiver. Again the deceiver cannot predict how this new clue will be interpreted. In G reception is intact but a competing signal's implications overwhelm the signal in interpretation and replace it.

The accidents which interrupt and corrupt a signal before it reaches its destination often resemble what communications theorists define as "noise." As Reese points out, strict adherence to the definition of noise in communications theory would restrict our labeling as noise only the random accidents between transmission and reception of the signal, i.e., signals B and C in our figure. Accidents in interpretation, or those which result from deliberate, competing signals, do not meet physicists' standards of randomness, though to the deceiver's plans they will be equally devastating.

Accidents in interpretation sometimes cannot be avoided. Since by definition deceivers wish to remain undetected, they must operate indirectly, at a discrete remove from their victims; they cannot risk overplaying their hand in order to guide the target's analysis. The target must inadvertently meet the deceiver halfway by figuring out what the evidence means for himself. In effect, the deceiver must have the connivance of the target to succeed at deception, and thus all deception includes an element of self-deception through the

target's active participation.

Two factors are especially pertinent to difficulties in predicting how an opponent will interpret a given clue: psychological perception and organizational processes. Heuer points out that perception is more than a passive response to stimuli. It is an active constructing of reality wherein one selects, arranges, and attaches meanings to certain stimuli from the great mass available. Individuals do this on the basis of rules and conventions learned over time. One's past experiences and training inevitably set in place a "mind set" which in Heuer's words is "akin to a screen or lens through which we perceive the world."<sup>5</sup> A signal picked up by the target's sensors intact may be misperceived as it passes through the mind set of the individual or group assigned to understand what it means. What seems to the deceiver a clear and logical inference anyone would draw from a clue may be filtered out or twisted by the target.

A second source of misinterpretations is the effect organizations may have on the interpretation of data. Sherwin reminds us that intelligence organizations are the initial targets of deception. Ultimately a decision-maker must be led into acting against his best interests for the deception to succeed, but this first involves fooling the organization which receives and interprets the signals which go into an intelligence evaluation. In addition to the perceptual filters individuals bring to their tasks, the organization is likely to have norms and assumptions about what certain things mean or

portend. In effect the organization often socializes its members into a group viewpoint, which if known can be played on by a deceiver.

Should an analyst resist the prevailing views of the group and raise a new possibility, another aspect of organizational life may prevent his dissent from succeeding. Despite a commitment to objectivity, most hierarchical organizations cannot escape seeing the importance of an interpretation as a function of the status of the person espousing it. Dissent from the top commands more attention than dissent from a low-level analyst, no matter how well-founded his suspicions. The pressures toward group consensus in any organization tend to eliminate eccentricity, including an occasional offbeat but correct view.

These group processes can slant, block, or filter the meanings assigned by a group to a series of clues. If a deceiver's signals run aground on some bureaucratic sensitivity, or on the "mind set" of the organization, he will fail to shape his target's beliefs.

Further difficulties arise from the fact that even when a decision-maker is fooled by a deception, he may not always act on his false beliefs. Contingencies can intervene which prevent the target from taking the action the deceiver is trying to elicit. On the one hand, new information or pressures may impinge on a decision-maker, causing him to act in unexpected ways not consistent with his deceptively-induced beliefs. Bureaucratic competition for scarce resources, for example, sometimes prevents carrying out activities which in all other respects seem inevitable.

On the other hand, in the mere passage of time from the point at which the deceiver planned and executed his series of signals until the target must take action, the situation may have changed and become something quite different. The original clues, once convincing and incorporated into the target's interpretation, may not elicit the expected action if events overtake them in the meantime. Then again chance in its many forms, e.g., bad weather or misplaced orders, can intervene to prevent action otherwise intended.

#### Advantages of the Deceiver

In practice deceptions usually succeed. They aid the deceiver's cause even if they do not go strictly according to plan.

Listing these many difficulties suggests that deceptions should seldom work, and yet the evidence available to us shows that they usually do. In part this paradoxical outcome may be an artifact of the familiar bias toward only documenting success. Bungled deceptions rarely appear in a deceiver's historical record, and they can seldom be proven after the fact by the target. We should search out and study more instances of deception failures to help overcome this bias. In the meantime, however, the records we do have suggest additional factors which help explain why deceptions succeed despite the difficulties we have identified. Some powerful elements in the

relationship between adversaries, in human perception, and in the environment play into the deceiver's hands.

One source of this advantage is embedded in the basic goals of hostile competition. Each adversary eagerly seeks out information about the other, while at the same time trying to deny access to information about itself. By opening up channels to the outside, and particularly to his opponent when possible, the adversary also opens himself up to being deceived via those channels. Although raw data about the enemy and the situation may flow into intelligence centers in enormous volume, highly reliable information is often scarce. A competitor is not able to dismiss information which may be true and which portends serious consequences. This puts the benefit of the doubt about the validity of such information on the side of the deceiver, for it ensures his deceptive clues a hearing by his target.

On balance, the processes of human perception and cognition provide a second source of advantage for the deceiver. While a few patterns in human thought favor the target, particularly in cases where the deceiver must change the target's mind, most of these patterns appear to conspire against the target. He is more often betrayed than served by his own processes of thought.

Psychologists characterize perception and cognition as organizing activities. Making what seems chaotic into a coherent, orderly, and at least partially predictable pattern is basic to human thought. The quantities of stimuli and types of information around us would overwhelm the senses were they

not selectively ordered by perceptual processing. The stimuli which do pass through the filters of our senses are recognized and categorized using concepts evolved from past experience. The meaning assigned to any one stimulus depends in part on the meanings of the other events, objects, or ideas which exist with it and form its context. In Sarbin's view the best analogy for understanding human thought processes is the creation of a narrative which ties together the disparate elements into a plot. By plotting a story which explains events chronologically, individuals keep the sense that they know with some confidence "what comes next" and can on this basis plan for the future. The drive for coherence is not a perfect process, however. Inevitably simplifications result in the loss of some information. The mind follows certain rules of convenience, sometimes called biases, which are not always optimal ways of sorting out information. Often these biases favor the deceiver.

The Appendix summarizes Heuer's discussion of cognitive and perceptual biases relevant to deception. Here we consider briefly why deceivers tend to profit from most of these patterns.

According to Heuer, the conclusion which emerges from considering these biases is that initial impressions are extremely important in that they shape all subsequent understandings of an event. Apparently the mind works by taking incremental steps: what we first learn about a topic becomes the touchstone against which each new datum is compared.

While some change in the overall concept does result from these later inputs, it is the persistence of the initial formulation and the resistance to changing it which are the striking features of the perceptual process. Five of the eleven biases Heuer describes converge to put a target of deception at the mercy of his initial impressions if they are reinforced by a deceiver: expectations shape what we in fact perceive; perceptions are quick to form but resistant to change; initially ambiguous perceptions delay the ability to clarify an assessment even when clear-cut evidence becomes available; estimates of the probability of some future event cluster around an initial starting point and resist radical alteration; and even after evidence has been completely discredited, the impressions based on it often persist and shape one's thinking. This convergence on the psychological importance of first exposure and the presumptions brought to data suggests why studies consistently find that M-1 deception, wherein a deceiver reinforces his target's existing views, are the most commonly tried, the most powerful, and the most likely to succeed of the deception variants. Barton Whaley's findings provide telling support for this: of 68 cases of strategic interaction he studied, he found that 79% of them succeeded by reinforcing what the target expected.<sup>6</sup>

We have seen how a deceiver profits from a target's eagerness for information and from many of the biases in human thought. He also benefits from a third factor, the effects of inherent uncertainties. Especially in competitions where



virtually all data are ambiguous and to some degree suspect, so often the case in war, the situation forgives most of the mistakes a deceiver makes. For example, security leaks, a major kind of mistake, seldom destroy a deception. If the deceiver's true plans, or the fact that deception is afoot, reaches a target, evidence suggests this is often not fatal to the deceiver's hopes. To explain this counterintuitive finding we must adopt the target's perspective: faced with an array of evidence which can rarely be documented as completely reliable, he must use more-or-less ambiguous data. Leaks to him must seem just another species of potentially true or potentially false signals. Even leaks which come from well-placed sources or over channels which are usually reliable must still jostle and compete against the range of alternatives the target's evidence supports. What seems to the deceiver a glaringly bright give-away often seems to the target either too good to be true or only one more among his many grey-colored clues.

Two psychological tendencies we have already mentioned contribute to the less-than-disastrous impact on most deceptions of security leaks. A leak is a new piece of evidence which contradicts or calls into question a previous assessment. Both the bias toward fitting new evidence into existing theories, even if it means twisting the new evidence to fit, and the bias toward maintaining one's impressions despite the subsequent discrediting of their source, tend to undercut the impact of a leak's new evidence.

A final advantage the deceiver holds is that although deception almost always inflicts costs on the target, attempting it entails few penalties for the deceiver even if it does not come off as planned. If the target is deceived he will probably act in a manner detrimental to his own interests; if he resists being taken in by the deception, he must still devote time and resources to evaluating the evidence and establishing probabilities for the future from the mass of clues. Trying deception, on the other hand, is often inexpensive because most illusions consume few of the total available resources. Failure, even being caught red-handed, does not prevent future successes at deception against the same target. The price of failure does entail the destruction of some "assets" for deception such as double agents or covert channels which are "blown," but these are less net losses than they are the foregoing of future benefits. The deceiver is always cushioned by the elemental fact that he knows the truth of his own intentions, and thus what is true from what is deceptive. The target does not and cannot with certainty know this, and the investment necessary to sort through yet another level of complexity introduced by deception falls with unequal force on the target's side.

#### Advantage of the Offensive

Being on the offense provides a better position for succeeding at deception than being on the defense. This is

particularly true in the early stages of an attack. Defensive deception, however, can be effective under the right circumstances.

It is reasonable to argue that being on the offensive provides a better position for succeeding at deception than being on the defensive. The basis for this view is that the initiator of military action is defining the nature and timing of the encounter and thereby has a greater degree of control over it at the outset. Because he knows what the truth will be--i.e., the location, timing, and manner of the planned attack--he can better orchestrate the dissemination of untruth than the defender who, in a sense, has no similar "truth" of his own providing a baseline for devising untruths. The defender obviously knows what he wants to defend, but he remains more or less uncertain as to specifically when and where he will be challenged by an attacker. He is also probably uncertain as to the magnitude and kind of attack he will face.

The attacker's deception advantage is usually greatest in the early stages of his offensive campaign. Once the campaign is well on its way, the situation often does not remain stable long enough for the attacker to devise and implement deception. A classic illustration is the relative non-use of strategic deception by the Allies after the Normandy breakout. The rapidly changing strategic situation between September 1944 and May 1945 was not conducive to the play of deception.

While being on the defense may not be conducive to engaging in deception, it would be wrong to say that defensive

deceptions cannot occur. They can be very effective under the right circumstances, especially given adequate time and resources. The defending party may attempt, e.g., to lay inviting axes of advance for enemy ground forces while remaining ready to ambush them should they take the bait. If the defender fears enemy bomber or missile strikes, he can also engage in extensive camouflage and decoy aimed at drawing enemy weapons away from high value targets to dummy sites instead. The British did this in 1940-1941, with limited results since they did not act to protect their assets until after war had begun. Their experience illustrates that defensive deceptions--at least of that type--have the highest chance for success if they are undertaken before the need for them is obvious because by then the time and resources needed to implement them may not be sufficient.

#### Astuteness

Deceivers who act astutely can enhance the advantages they already enjoy from the dynamics of deceptive interaction.

Cleverness on the deceiver's part can reinforce his chances of successfully deceiving his adversary. Certain behaviors distinguish expert deceivers from their mediocre counterparts. Experts seem to share a turn of mind useful for predicting the reactions of others, and they understand the demands deception imposes on them.

The most successful deceivers rely on some individuals who have acumen, an ability to "de-center" or step outside one's own viewpoint into the mind-set of an opponent. Someone with a keen sense of acumen can empathize closely enough with a target to predict with considerable confidence how he will see and respond to a given situation. British deception experts in World War II stressed the importance of individuals who could "get inside" the German mind and construct in their imagination how German analysts would piece together and interpret evidence.

Acumen seems to depend not only on logical ability; emotional and imaginative qualities play important parts. Thus in the British case during World War II, many of their most successful deception staffers brought their "flair" with them from diverse, non-military backgrounds in literary, theatrical, and business fields. Sarbin suggests that although it may be difficult, conceivably one could develop means to identify persons gifted with acumen, on the theory that this trait would be as valuable for counterdeception as it has proven to deceivers in the past.

Assuming a potential deceiver can bring to bear keen insights into the perceptions of his victim, how should he proceed in order to maximize his chances of success? Deciding what are the target's basic goals would seem to be a natural starting point. Knowing his goals should facilitate predicting the options to which he will best respond. The deceiver should send clues which give impressions consistent with the target's

goals, for these, as we have discussed above, he will most readily recognize and believe. If, as Moose suggests, one side's goals are directed toward preserving the status quo, the other side can predict they will be especially sensitive to signs that the current situation is stable. A clever deceiver should then provide those signs while preparing to disrupt that stability. At the level of generality of change vs. status quo, it appears that either an ambiguity-increasing or a misleading deception would accomplish the deceiver's object: if the target is confused he is likely to seize excuses to delay decision and action until he receives clarification; if he is misled by appearances that the deceiver acquiesces in the status quo, he will likewise do nothing. As elaborated by Reese in his application of game theory to deception, doing nothing until the situation clears is often a fatally attractive option which leads to one's being surprised.

Beyond concerning himself with a target's goals, an astute deceiver should try to determine his target's beliefs and expectations vis à vis the impending encounter. As emphasized earlier, a deceiver has a marked advantage if he spins a tale which a target is already predisposed to believe. Experts at deception strike a balance between keeping their deception subtle enough so as not to arouse the target's suspicions, and intervening vigorously enough to have the desired reinforcing effect.

The greatest demands are made on a deceiver's astuteness if he must change a target's beliefs. Deceivers here should

sequence their clues in a way which aims to shake the target's initial ideas severely enough that he "reopens the case" in his mind. By overcoming the tendency to assimilate new evidence to existing views with an initial large, compelling piece of evidence, the deceiver may force the target to reorient his views. Additional corroborating clues will then help to build up a plausible scenario of the deceiver's choice. The British "Mincemeat" ruse during World War II is an example of this sequencing to change the target's mind: confronted by a drowned courier with plans suggesting invasion sites on Sardinia, Hitler and his generals deployed forces away from Sicily, the real site, even though they had initially guessed correctly where the invasion would come.

It seems paradoxical but true that deceivers seeking to change a target's views should also aim to make him vigilant, even though that very vigilance may be instrumental in a target's rejecting a deceiver's false tale. Why this is so requires distinguishing three emotional states associated with making important decisions.

The first of these is relaxation: an individual feels no tension because no such decision is required of him. The second is that of moderate tension, or vigilance: some tension arises from the need for a decision, but it remains moderate as long as the individual believes he has adequate time to evaluate alternatives before deciding on one. The third state is high tension, or rigidity. Here the individual feels great stress because time seems inadequate to properly evaluate alternatives.

Psychologists argue that individuals are most apt to follow their predispositions in either the first or the third emotional states: when they are relaxed, or when they are very tense. In the first case, facing no important decision, the individual sees no disadvantage in giving head to his predispositions. Pressed for important decisions in a hurry, on the other hand, individuals fall prey to what they consciously or subconsciously choose to see. It is the second state of moderate tension, or vigilance, that elicits responses most likely to overcome predispositions. Individuals are then evidently most open-minded as they seek out information to make a rational decision. In short, deceivers should confront a target with the need to make an important decision but should avoid placing the target in a crisis situation if the aim is to change the target's beliefs.

In "Operation Mincemeat" the British organized their clues to suggest that Sardinia would be invaded in the coming months, but not immediately. Hitler and his intelligence staffs were given reason to doubt their expectations about Sicily. They had time to reassess the situation and put together an alternative scenario incorporating Sardinia. Had the British rushed them into crisis-decision-making, they would probably not have shifted their forces so cooperatively.

In other circumstances the astute deceiver will decide that he gains most by generating just such a crisis in decision-making for the target. Looking at how organizations function, Sherwin notes that increasing stress improves an organization's ability to process information only to a certain point.



Thereafter the internal system collapses and the organization cannot systematically process data. This "fibrillation" could be very useful to a deceiver who needs to paralyze the target's intelligence and command structures while he moves quickly against him.

However, the cost the deceiver pays for deliberately provoking the false perception of crisis by his opponent is some inability to predict his responses accurately. What the deceiver knows about a target's normal behavior during steady state periods is undercut when the target moves into crisis and shifts to extraordinary coping behavior. It may be advantageous to a deceiver to risk this unpredictability in order to reduce the target organization's efficiency. Many of the distracting deceptions connected with the Normandy landings, for example, such as dummy paratroops and multiple fake landing sites, served to stretch and overload the ability of German intelligence to sort out and respond to threat. There is some danger, though, that by generating crisis the deceiver will find himself facing some unexpected response which was saved just for such exigencies. Perhaps the key to assessing this risk is the quality of the deceiver's channels of information to the target, in particular the feedback channels we will discuss below.

In addition to seeing things through the target's eyes, assessing his goals, and determining how much time pressure a victim should face, astute deceivers recognize that they should follow certain rules to maximize their chances of succeeding.

Past deception experts have left primers which distill the lessons they learned from experience. If not applied too rigidly, these lessons continue to be useful. For example, a scenario for deception on a strategic scale, which by definition is complex and persists for at least several weeks, must remain plausible to the target for as long as it is running. One aspect of establishing plausibility is making sure the target obtains confirmation of the crucial deceptive elements from various and reliable sources. Another is to ensure the scenario adapts to changing circumstances and evolves in a "real-life" way. The best deceivers are sensitive enough not to overplay their hand: they knit false clues into a web of many truths which can be independently verified and found to "ring true." The more data points are determined by the target to be true, the more likely he is to twist or ignore the remaining discrepant ones to fit his hypothesis. In addition, clever deceivers try to sabotage as many sources of disconfirming evidence as possible, and they strive to lay before the target proof that they have the capabilities to carry out the operations the deceptive scenario suggests.

This advice reflects an intuitive understanding of several psychological biases people bring to the analysis of evidence (see Appendix) on psychological factors in deception. In particular, deception experts seek to play on individuals' over-sensitivity to consistency. Since people will believe a small sample of consistent data more readily than a larger, more statistically reliable sample which is inconsistent, deceivers aim for a variety of clues which all reinforce and support one

scenario. However, there is another side to the need for consistency. People also tend to under-estimate the importance of missing data in an array of evidence. What is there blinds them to the significance of what is not. The clever deceiver realizes that he need not, and probably should not, try to tie up every loose end and hypothetical possibility in his scenario. The target will work with the evidence he has and will tend to discount what is missing. An elaborate airtight case might excite suspicion if it looked "too good to be true," that is too consistent, and it may not allow sufficient flexibility to weave in chance events as they occur. Resisting the temptation to go too far in one's desire to ensure the target makes the right deductions is one of the hallmarks of astute deceivers.

#### Feedback

In strategic deception feedback is the deceiver's most valuable asset. It forms the basis of the most astute deceptions.

In order to carry out an extended deception one must adapt it to the changes inevitable in an evolving situation. The deceiver's most valuable asset for doing this is feedback. Feedback is accurate and timely information about an adversary's reactions. It can be direct or indirect; the former is more powerful, the latter more common.

Indirect feedback simply consists of observing how the other side responds to an action or event. It is available to anyone who systematically observes any sort of interaction including deception. One acts and waits for visible signs of the opponent's reactions. If an action is specifically designed to test the reaction, indirect feedback is usually better focused and likely to be more useful in characterizing an opponent.

For strategic deception, however, a more precise form of feedback is usually desirable. Since military adversaries cover up their own reactions and simulate appearances to suit their needs, visible reactions can be unreliable. The side which achieves a reliable covert channel into his opponent's camp over which feedback can flow has, as spy novels often portray, a most precious advantage. This is direct feedback consisting of systems such as ULTRA in World War II or well-placed espionage agents. They pass information which in effect short-circuits the normal channels between sides. Adversaries as a matter of course eagerly seek such useful channels because the information obtained is usually more complete and unambiguous than indirect feedback would be. However, as the fate of most spies demonstrates, direct channels are also inherently risky and usually temporary.

In addition to providing fuller, more reliable insight into the enemy's camp, direct feedback may allow the deceiver to risk lying more often and get away with it. Typically, the deceiver must use many true signals in which a few lies are

embedded in order to protect the impression of reliability his target has of the channels. If the target finds the information from a channel is false too often, i.e., more than the rate of error normal for such channels, he will stop relying on it. Direct feedback tells the deceiver quickly which of his lies the target accepts and which he questions, what he finds suspicious or inexplicable, and what he swallows without qualm. Thus the deceiver can at once back up lies which are questioned, or soft-pedal them, so that numerous lies can be passed and protected without damaging the target's perception of how reliable the channel is. The British use of their double agent system in World War II is an extreme example of the rich possibilities for such a direct feedback system and its potential for passing lies. Many of the dangers from uncontrolled channels and from random accidents in deception scenarios can be eliminated by direct feedback because these hitches can be detected and corrected quickly, before an alternative scenario has taken hold in the target's mind. Furthermore, direct feedback prevents a target from ambushing the deceiver, which removes the largest threat the deceiver faces.

A third aspect of direct feedback's value for deception lies in its ability to overcome the unpredictability associated with crisis. Moose argues that indirect feedback may well suffice adversaries in situations where a competitive system persists over a fairly long period of time. When change is gradual and the parts of the system interact in stable ways, predictions of what the other side will do based on

observations of past behavior can be quite accurate. Stability not only implies peaceful conditions; prolonged conflict between evenly matched adversaries could become similarly predictable.

However, in times of transition or crisis, such as a surprise attack or warfare between opponents with rapidly shifting relative strengths, each side replaces its usual modes of operation with emergency routines. It no longer acts "normally." New pressures generate extraordinary exertions or desperate expedients, and the rapid changes each side undergoes prevent prediction based on observing the responses of the adversary. By the time one observes a response the opponent may have changed in some crucial way and will not or cannot respond that way again in the future. Thus in crises or transitions, when equilibrium and stability are lost, direct feedback with its shorter response time offers the only realistic means to predict the opponent's next likely move. By allowing a deceiver to hold his fingers on the pulse of his target even while the latter is changing rapidly, direct feedback allows the deceiver to keep up, providing new clues as needed to prolong and preserve the scenario's plausibility.

Deceivers themselves have viewed direct feedback as crucial for their success in elaborate, long-term deceptions. John Bevan, head of the British deception effort in London after 1943, credited their unusually intimate feedback through ULTRA with supporting the complex, multi-layered deceptions the British launched against the Germans. Often by coordinating information

from ULTRA with their extensive network of turned German agents, British deceivers could incorporate the Germans' unexpected interpretations of their signals or sudden shifts in events into the deception scenario. This ability to touch on additional true reference points enhanced credibility considerably. This feedback also allowed the British to back off when a story wore thin, which prevented the enemy firmly concluding that deception was at hand, and allowed the deceivers to salvage their precious double agents and other resources for further deceptions.

The contrast between the sophisticated Allied strategic deceptions in the European theatre during World War II and the relatively simple American efforts in the Pacific promises to be instructive as more data on the Pacific cases becomes available. Certainly one explanation for these differences was the quality of feedback adversaries in each theatre achieved. In Europe the British, later the Allies, had unusually good intelligence, perhaps so good it is unlikely to be matched again, while German intelligence degenerated quickly to become unusually poor. In the Pacific, intelligence may have been more evenly matched until close to the end, but even with MAGIC, the Allies did not have direct feedback from Japan comparable to ULTRA. Pacific strategic deceptions appear, on the basis of initial study, to have been more tentative, less opportunistic in building on evolving events, and considerably more cautious as a consequence of persistent uncertainties about how the Japanese were responding. Observational feedback, e.g., reports on Japanese troop movements and ship positions, and the lucky

capture of Japanese documents guided American deceivers in operations such as WEDLOCK and BLUEBIRD, both designed to protect the truth about where American forces would strike next. The importance of direct feedback for perpetrating strategic deception relative to other factors which differed between the European and Pacific Theatres, such as familiarity with the enemy culture and language, or the physical size of the area of operations, awaits further investigation.

### Counterdeception

Countering deception is extremely difficult, but success need not always require detecting deception.

Countering deception is traditionally conceived of as a two-step process of first detecting and then foiling deception. This discussion will focus on each step in turn after presenting a few observations on the counter-deception problem in general.

The difficulty countering deception. Barton Whaley has analyzed 68 cases of attempted strategic military surprise occurring between 1914 and 1968. Fifty-seven of the instances involved resort to deception, and of this group, 50 (or 88 percent) resulted in some degree of surprise. It is necessary to emphasize that the cases Whaley studied seem skewed in the direction of successful surprise; nevertheless, Whaley's data suggest that deception may be very difficult to foil, especially since the target in each case had the benefit of at least some warning.



This conclusion is not surprising since the deception variants which seem to occur most often--the M-1 and A types--are those where the target is the most cooperative. The difficulty of countering M-1 deceptions is that the target is inclined to accept the perpetrated lies before the deception starts; his perceptual and cognitive biases militate against his rejecting them. It is noteworthy that 79 percent of Whaley's cases involved exploiting a target's preconceptions.

In A deceptions, the deceiver need only send lies which are plausible and consequential to the target's interests. If the lies go through to the target, the latter's desire to make rational or good decisions helps guarantee that he will not ignore the deceptive information. If he delays making a final choice in order to await additional clarifying data, he surrenders the initiative and leaves himself open to surprise. If he hedges by distributing resources to cover plausible contingencies, he faces the prospect that his resources will be inadequate to deal with the contingency on which the deceiver will act.

Only in M-2 deceptions does an initial advantage lie with target. His perceptual and cognitive biases incline him from the start to ignore deceptive messages and to doubt their veracity.

Detecting deception. Sources such as ULTRA or an agent in the enemy's headquarters are probably the best ways to establish whether that enemy is being deceitful. These sources, however, are generally unavailable and certainly not foolproof. ULTRA,

e.g., did not prevent the Allies from being surprised by Germany's Ardennes offensive during the winter of 1944 (the Battle of the Bulge).

Any state's attempt to harness more mundane intelligence assets to the counter-deception problem must be done delicately. Consistent with the psychological arguments we have presented earlier, it is highly probable that attempts to sensitize intelligence analysts to the prospect of deception will incline them to find "deception" when it isn't there. Indeed, as Heuer suggests, intelligence analysts are generally predisposed to perceive deception without any encouragement to look for it. He reasons:

Instances of successful deception are far easier to recall than cases in which deception was not employed under similar circumstances and this sensitizes [an intelligence analyst] to the possibility of deception. [Analysts] are [also] attracted to deception as an explanation for otherwise incongruous events because the deception explanation allows [them] to impose order and reason on a disorderly world, and because it enables [them] to attribute deviousness and malevolence to...enemies. These factors sometimes cause [analysts] to perceive deception when it is not really present.<sup>7</sup>

Heuer's conclusion parallels that of Sarbin who argues, in effect, that to encourage an analyst to look for deception will probably lead him to subject intelligence data to particularly detailed or fine-grained scrutiny. "To use a more fine-grained... procedure has an important implication: the observer will read into the behavior [of actor(s) being observed] the interpretation that the actor(s) are being deliberate, rather than spontaneous;

the instantiation 'being deliberate' rather than 'spontaneous' is more likely to be followed by the attribution of deception to the observed sequence."<sup>8</sup>

In short, sensitizing analysts to the possibility of deception can have pernicious effects, including a high false alarm rate and a resulting "cry wolf" syndrome where true deception is discounted. It can also lead to a situation where analysts, no longer sure what they should accept as true, impose such rigid standards of proof that they suppress either the freeplay of intuition so much a part of intelligence analysis or the flow of intelligence from analysts to decision-makers. Prior to the Cuban Missile Crisis, e.g., John McCone, CIA Director, suspected the USSR was emplacing missiles into Cuba and alerted President Kennedy several times. The President grew impatient with McCone when the latter could produce no hard evidence. McCone reacted by drawing back; despite his suspicions he did not raise the issue again until the U-2 photos provided clear proof.

Suppressing intuition for the sake of clear-cut proof can be particularly unfortunate if, as Sarbin contends, a variant of intuition, acumen, is the key to discovering deception.

Prediction by acumen, [he writes,] is the stock in trade of persons who can penetrate the masks or expose the lie of the antagonist. [They] do this...through empathic skill....Literary sources abound in examples of this quality: Chesterton's gifted sleuth Father Brown and the narrator in Edgar Allen Poe's detective stories made their predictions of the behavior of others through 'taking the role of the other.'<sup>9</sup>

Simple controlled experiments have established that some people have a talent for "de-centering" or "taking the role of the other," but one should hesitate, Sarbin contends, "to select persons as deception analysts exclusively on the basis of current research." It also remains to be seen whether a person selected for acumen in interpersonal relations could apply his skill to good effect in analyzing international political or military situations.

Less difficult than finding individuals with proper acumen is the institutionalization of intelligence procedures consistent with counter-deception. These procedures are usually recommended for avoiding intelligence surprise in general. They include methods for generating alternative hypotheses of enemy behavior against which evidence is sought and evaluated. A devil's advocate is one well-known method; another is competing analyses by different agencies which are given access to the same information.

It is not enough, of course, for an intelligence organization to suspect strongly or detect traces of deception. (Indeed, the possibility of deception often readily comes to mind in ambiguity producing cases.) A target must still separate the real from the lie. History is replete with cases where the lie has been accepted as real and where truth has been deemed to be deception. A classic example occurred prior to the Soviet Summer offensive of 22 June 1944. Working to convince the Germans that the attack would be concentrated against Army Group North Ukraine, the Soviets actually prepared to strike Army Group Center instead.

Between 30 May and 22 June signs of a Soviet buildup off Army Group Center "multiplied rapidly as the deployment went into high gear, but they were not enough to divert the OKH's [i.e., the German Army's High Command] attention from Army Group North Ukraine....The [Wehrmacht's] Eastern Intelligence Branch dismissed the activity opposite Army Group Center as 'apparently a deception.'"<sup>10</sup>

As a matter of course, intelligence agencies should seek to draw responses from a suspected deceiver which can help confirm or deny deceptive intent. For instance, by indicating rejection of a suspected lie, a target may trigger a measurable increase in deceiver activity aimed at reinforcing the lie. The increase should heighten suspicion that deception is afoot. Shortly after the Normandy landing, e.g., the British learned that Hitler had ordered troops transferred from the Calais to the Normandy areas. The British feared that Hitler no longer viewed the Calais area as the ultimate main point of attack and Normandy as only a feint. Controlling all German spies in the UK, they had one send a special wireless message on 9 June to his German paymasters. The agent transmitted for two hours--a period of highly unusual length--as he argued that a large landing would soon occur at Calais. The message was instrumental in Hitler's cancelling of the troop transfer, but its special nature and length constituted a marked increase in the

British deception effort which could have aroused German suspicions.\*

Foiling or deterring deception. A target may pursue two courses of action upon detecting deception. He can reveal his discovery to the deceiver, thereby forcing him to abandon the deception and possibly also the military operation supported by it. The target can also try to keep the discovery a secret, stringing the deceiver along in the hope of ambushing the latter's forces.

The above actions are premised on first detecting deception, but it also theoretically is possible to foil a (potential) deceiver without proof or even evidence of deception. The most realistic way a (potential) target can do this is to remain

---

\*Some historians imply that it should have aroused German suspicions. Sefton Delmar, for instance, notes that the agent's transmission was of such length that, had it "been the genuine product of an enemy agent, the [British] Radio Security Service would have had ample time to locate its transmitter and arrest its operators several times over." (Emphasis in original.) Since German and British radio-direction finding techniques were comparable, one can only wonder if anyone in Germany did question how their agent got away with transmitting for so long. See Delmar, The Counterfeit Spy (New York: Harper and Row, 1971). p. 187.

unpredictable, for uncertainty about whether a target is taking the bait, or how a target will deploy forces and react to an attack, can significantly increase a deceiver's fear of ambush. As suggested in Reese's application of game theory to deception, if a rational deceiver rates the costs and prospects of ambush high enough, he will probably be deterred from initiating or continuing deception. Ironically a (potential) target could be well-served by engaging in its own deception in order to increase enemy uncertainties and thereby decrease the enemy's probability of resorting to deception.

It is consistent with the above emphasis on unpredictability that deterring or foiling deception is often a byproduct of maintaining the strategic military initiative. While it would be folly to initiate an attack merely to avoid being deceived, the facts remain that strategic deceptions take weeks to implement and usually require that the victim be passive if not predictable during that time. The reason is that a deceiver is usually thrown off balance, and his plans overtaken by events, if the victim engages in rapid large-scale or unpredictable changes of behavior. These are precisely the kinds of changes which occur when a state is pressing the strategic initiative.

In sum, counter-deception is extremely difficult. It is not enough merely to alert one's analysts to the possibility of deception, for such action may be dysfunctional. The institutional mechanisms (such as devil's advocates) so often suggested for avoiding strategic surprise are obviously and

directly relevant for counter-deception. States fearful of being deception targets should look for opportunities to draw a response from a potential deceiver which helps confirm whether or not deception is afoot. Even when deception is not evidenced or ongoing, it may be possible to deter it by heightening a prospective deceiver's fears of ambush.



## CHAPTER FOUR

### CONCLUSION

We offer here two final thoughts about the utility of deception. One is that deception's contribution to the outcome of any military campaign remains impossible to measure with scientific precision. Such precision would require verifiable answers to the following questions:

- What did a target believe before deception was attempted?
- What did he come to believe because of the deception?
- What did he decide to do because of his deception-induced beliefs?
- What was the relative impact of those decisions and actions on the military outcome when compared to other factors such as generalship, quantity and quality of weapons, material resources, troop morale, and the like?

Each of these questions is progressively more difficult to answer. The second and third questions are especially difficult in cases where there is only a fine line between perpetrated deception and target self-deception, or between perpetrated ambiguity and the ambiguity inherent in any wartime situation. The fourth question restates an analytical problem facing not only students of deception but also all strategic planners and

military historians. Until one of them devises a model or formula for measuring accurately the impact of varying factors contributing to victory or defeat, and until adequate data becomes available to apply such a model, it will remain impossible to estimate deception's relative impact with other than rough subjective precision.

With the above as a caveat, it is the considered view of the NPS Deception Working Group that deception is a powerful tool, particularly in the hands of an astute practitioner. Barton Whaley's data, while it may seem skewed towards cases of successful deception and surprise, supports that conclusion. The logic of the deception situation does so as well. The deceiver, after all, knows the truth, and he can assume his adversary will search for its indicators. As a result, the deceiver can expect the victim to pick up some of the signals intended to mislead or confuse. Should they be ignored, dismissed, or misinterpreted, the deceiver is probably not worse off. Should they be interpreted as he intends, the deceiver stands to gain. The target must pay attention even to scenarios which he suspects to be untrue if they are plausible and consequential to his interests. Although the target may ultimately choose not to act on them, the additional time he spends evaluating deceptive scenarios or searching for further information should benefit his foe.

## APPENDIX

### REVIEW OF BIASES AND THEIR IMPLICATIONS FOR DECEPTION

BIAS	IMPLICATION
<hr/> <b>Perceptual Biases</b> <hr/>	
Perceptions are influenced by expectations. More information, and more unambiguous information is needed to recognize an unexpected phenomenon than an expected one.	It is far easier to reinforce a target's existing preconceptions than to change them.
Perceptions are quick to form but resistant to change. Once an impression has been formed about an object, event or situation, one is biased toward continuing to perceive it in the same way.	It is far easier to reinforce a target's existing preconceptions than to change them. Ability to rationalize contradictory information may offset risks of security leaks or uncontrolled channels.
Initial exposure to ambiguous or blurred stimuli interferes with accurate perception even after more and better information becomes available.	Impact of information can be affected by the sequence used in feeding it to a target.
<hr/> <b>Biases in Estimating Probabilities</b> <hr/>	
Probability estimates are influenced by availability--how easily one can imagine an event or remember instances of an event.	Employees of watch offices will generally overestimate the probability of whatever they are watching for. This leads to the cry wolf syndrome. Cases of deception are more memorable, hence more available, than instances in which deception was not employed.
Probability estimates are anchored by some natural starting point, then adjusted incrementally in response to new information or further analysis. Normally they are not adjusted enough.	It is easier to reinforce a target's existing preconceptions than to change them.

In translating subjective feelings of certainty into a probability estimate, people are often overconfident about how much they know.

Overconfidence exacerbates the impact of all the biases, as it leads to self-satisfaction and lessening of efforts to improve judgment.

---

### Biases in Evaluating Evidence

---

People have more confidence in conclusions drawn from a small body of consistent data than from a larger body of less consistent information.

Deceiver should control as many information channels as possible to reduce amount of discrepant information available to the target. Deception can be effective even with a small amount of information.

People have difficulty factoring the absence of evidence into their judgments.

For the deception planner, errors of omission will be less serious than errors of commission. To detect deception, analyze what inferences can be drawn from fact that some evidence is not observed.

Impressions tend to persist even after the evidence on which they are based has been fully discredited. You cannot "unring" a bell.

Consequences of a security leak may not be as serious as might otherwise be expected.

---

### Biases in Perceiving Causality

---

Events are seen as part of an orderly, causal pattern. Randomness, accident and error tend to be rejected as explanations for observed events. Extent to which other people or countries pursue a coherent, rational, goal-maximizing policy is overestimated.

As a causal explanation, deception is intrinsically satisfying because it is so orderly and rational.

Behavior of others is attributed to the nature of the person or country, while our own behavior is attributed to the nature of the situation in which we find ourselves.

It is satisfying to attribute deviousness and malevolence to our enemies, and if they are devious and malevolent, of course they will engage in deception.

## REFERENCES

<sup>1</sup>Barton Whaley, Codeword Barbarossa (Cambridge, Mass.: MIT Press, 1973), p.242.

<sup>2</sup>Scott A. Boorman, "Deception in Chinese Strategy," The Military and Political Power in China in the 1970's, edited by William W. Whitson, (NY: Praeger, 1972), pp. 315-316.

<sup>3</sup>William R. Harris, "On Countering Strategic Deception," (Draft R-1230-ARPA; Santa Monica: Rand Corporation, 1973).

<sup>4</sup>Herbert Goldhamer, "Reality and Belief in Military Affairs: A First Draft" (June 1977), edited by Joan Goldhamer (R-2448-NA: Santa Monica: Rand Corporation, 1979), pp. 107-08.

<sup>5</sup>Richards J. Heuer, "Cognitive Factors in Deception and Counterdeception," in D.C. Daniel and K.L. Herbig et al., Multidisciplinary Perspectives on Military Deception (Technical report 56-80-012: Monterey, CA: Naval Postgraduate School, 1980), p. 52.

<sup>6</sup>Barton Whaley, Stratagem: Deception and Surprise in War (Unpublished manuscript; Cambridge, Mass: MIT, 1969).

<sup>7</sup>Heuer, p. 88.

<sup>8</sup>Theodore Sarbin, "On the Psychological Analysis of Counterdeception," in Daniel and Herbig et al., p. 139.

<sup>9</sup>Ibid., p. 128.

<sup>10</sup>Earl F. Ziemke, Stalingrad to Berlin: The German Defeat in the East (Washington, DC: US Army, Office of the Chief of Military History, 1968), p. 315. Ziemke is quoting from a German intelligence report.

# DISTRIBUTION

1. Defense Technical Information Center Cameron Station Alexandria, VA 22314	2
2. Dean of Research, Code 012 Naval Postgraduate School Monterey, CA 93940	1
3. Naval Postgraduate School Library Research Reports Division, Code 1424 Monterey, CA 93940	2
4. Office of Research Administration, Code 012A Naval Postgraduate School Monterey, CA 93940	1
5. Professor Katherine L. Herbig, Code 56 Naval Postgraduate School Monterey, CA 93940	30
6. Professor Donald C. Daniel, Code 56 Naval Postgraduate School Monterey, CA 93940	30
7. Dr. Theodore Sarbin, Code 56 Naval Postgraduate School Monterey, CA 93940	1
8. Professor Ronald G. Sherwin, Code 56 Naval Postgraduate School Monterey, CA 93940	1
9. Professor William Reese, Code 61 Naval Postgraduate School Monterey, CA 93940	1
10. Professor Paul H. Moose, Code 61 Naval Postgraduate School Monterey, CA 93940	1
11. Mr. Richard Heuer, Code 56 Naval Postgraduate School Monterey, CA 93940	1
12. Professor Pat Parker, Code 56 Naval Postgraduate School Monterey, CA 93940	1

13.	Mr. Andrew W. Marshall Director of Net Assessment Office of the Secretary of Defense Pentagon (Room 3A930) Washington, D.C. 20301	2
14.	Lt. Col. F.W. Giessler Office of the Director of Net Assessment Office of the Secretary of Defense Pentagon (Room 3A930) Washington, D.C. 20301	50
15.	Clare Fieldhouse CIA (DDO/SE) 4 Doo HQs Washington, D.C. 20505	1
16.	Lt. Col. A.L. Serman OJCS J3 (SOD) The Pentagon Washington, D.C. 20301	1
17.	Maj. Philip Ferguson DIA ATTN: DB-IE Washington, D.C. 20301	3
18.	Captain Robert Tolle CNO Executive Panel 2000 N. Beauregard St. Alexandria, VA 22311	1
19.	Mr. William Spahr OSR/SE/S CIA Washington, D.C. 20505	1
20.	Dr. Barton Whaley 38 Josiah Avenue San Francisco, CA 93112	1
21.	Maj. Gen. William A. Harris, ret. 206 B. Ruelle San Antonio, TX 78209	1
22.	Dr. Mary Walsh AMR/ORD CIA Washington, D.C., 20505	2
23.	Maj. Gen. William Baumer Box 1045 La Tolla, CA 92038	2
24.	Richard Betts 1775 Massachusetts Ave. N.W. Brookings Institution Washington, D.C. 20036	1

- |     |  |   |
|-----|--|---|
| 25. | Robert Jervis<br>Department of Political Science<br>Columbia University<br>New York, NY                              | 1 |
| 26. | Admiral B.R. Inman, USN<br>CIA<br>Washington, D.C. 20505   | 1 |
| 27. | Mr. Robert Mullins<br>Department of Government<br>The University of Texas at Austin<br>Austin, TX 78712              | 1 |
| 28. | Dr. J.D. Douglass, Jr.<br>System Planning Corporation<br>1500 Wilson Blvd.<br>Arlington, VA 22209                    | 1 |
| 29. | Commander<br>Combined Arms Combat Development Activity<br>ATZL-CAC-I (CPT Dan Lynn)<br>Ft. Leavenworth, Kansas 66027 | 1 |
| 30. | Capt. Ernest K. Beran<br>NQ ESC/D00C<br>Kelley AFB, TX 78243   | 1 |